

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES**

Applicant(s): Brian J. Reistad et al.
Appl. No.: 09/054,180
Conf. No.: 2217
Filed: April 1, 1998
Title: ELECTRONIC COMMERCE SYSTEM
Art Unit: 3621
Examiner: Firmin Backer
Docket No.: 115274-008 (Was 113948-064)

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPELLANTS' APPEAL BRIEF

Sir:

Appellants submit this Appeal Brief in support of the Notice of Appeal filed on April 13, 2004. This Appeal is taken from the Final Rejection dated November 13, 2004.

I. REAL PARTY IN INTEREST

Soverain Software LLC is the real party in interest of the above-identified patent application by virtue of an assignment to Connor Robert Patent Holdings LLC which subsequently became Soverain Software LLC.

II. RELATED APPEALS AND INTERFERENCES

To the best of Appellant's knowledge there are no pending appeals or interferences that will directly affect, have a bearing on, or that will be directly affected by, the Board's decision with respect to the above-identified Appeal.

III. STATUS OF CLAIMS

Claims 12-36 and 39-63 are pending in the Application. A copy of the appealed claims is attached in the Appendix. At present, claims 12-36 and 39-63 stand rejected under 35 U.S.C. §102(e) as being unpatentable over U.S. Patent No. 6,057,872 to Candelore. A copy of the Final Office Action and the prior art on which the rejection was based are included in the Supplemental Appendix.

09/09/2004 EAREGAY1 00000066 09054180

01 FC:1402

330.00 NP

IV. STATUS OF AMENDMENTS

There have been no amendments made in this case. A response traversing the Examiner's rejection was filed on September 30, 2003.

V. SUMMARY OF INVENTION

The invention relates to an electronic commerce system that enables automated negotiation and processing of on-line orders. The system ensures that final orders conform to advanced order acceptability criteria established by the seller, but allows for flexibility in defining the terms and conditions of transactions to satisfy the needs of the buyer.

Client computers, such as those operated by buyers who wish to purchase goods or services from a seller, negotiate with the electronic commerce system to arrive at a set of terms and conditions which are acceptable to both the buyer and the seller. The negotiation is conducted according to a protocol which is driven by the buyer, but where the final terms and conditions must be accepted by the electronic commerce system. Once the negotiation phase is complete, when both the electronic commerce system and the client have agreed on a set of terms and conditions, the client and the electronic commerce system enter into a transaction phase wherein the terms and conditions which were agreed upon during the negotiation phase are "captured", and an order for the desired goods or services is processed according to the agreed upon terms and conditions.

During the negotiation phase the client sends an order acceptance request message to a server associated with the electronic commerce system. The order acceptance request may include data identifying the buyer, the seller, the goods or services the buyer wishes to purchase, terms and conditions of a purchasing transaction, and so forth. The server processes the order acceptance request and generates a corresponding order acceptance response which is sent back to the client. The order acceptance response includes an amended version of the original order acceptance request sent by the client. The order acceptance response identifies which of the original terms and conditions meet the server's order acceptance criteria and which do not. The order acceptance response may also identify additional required terms and conditions that may have been omitted entirely from the original request. The order acceptance response may include alternative choices that may also be acceptable to the server or a menu of proposed replacement terms, or the like.

Upon receiving the order acceptance response, the client may abandon the transaction, incorporate the server's changes into a new order acceptance request or change the order acceptance request in other ways. The client and the server continue this negotiation process until either the client abandons the negotiation or the client and the server arrive at terms and conditions acceptable to the client and which meet the order acceptance criteria of the server.

When the terms and conditions are acceptable to the client the client can enter the transaction phase by indicating client approval to the server. If the order acceptance request is acceptable to the server, the server captures the order acceptance request for the client. Capturing the order acceptance request effectively ends the negotiation between the client and the server. Backend systems associated with the electronic commerce system then process the order according to the agreed upon terms and conditions and fulfill the order.

Thus, the electronic commerce system enables automatic negotiations between a buyer and a seller, or between a client computer operating on behalf of a buyer and a server computer operating on behalf of a seller, where the server computer includes software that enforces complex order acceptance criteria. The protocol associated with the invention enables the client computer and the server computer to efficiently negotiate toward a complete and acceptable order.

According to an aspect of the invention the order acceptance request message sent from the client to the server is a discrete message that may include a plurality of modular components. The individual integrity of each modular component of the order acceptance request message is protected by a cryptographic security code embedded within the modular component. For example an order acceptance request may include a digital coupon which the client obtained from a third party, or gift certificate, or some other message component such as a free shipping offer or the like, which would impact the transaction.

When the server computer receives an order acceptance request, the server authenticates the cryptographic security codes embedded in the modular components and processes the request in accordance with the authenticated modular components. The order acceptance response message sent from the server to the client may also comprise a discrete message made up at least in part of a plurality of modular components. Again, the individual integrity of each modular component of the order acceptance response message is protected by cryptographic security codes embedded within each modular component.

VI. ISSUE

Whether U.S. Patent No. 6,057,872 teaches every element of the invention as claimed in claim 12-36 and 39-63.

VII. GROUPING OF CLAIMS

Claims 12-36 and 39-63 stand or fall together.

VII. ARGUMENT

A. Legal Standards

“A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference.” Verdegall Bros. v. Union Oil Co. Of California, 814 F. 2d 628, 631, 2 U.S.P.Q. 2d 1051, 1053 (Fed. Cir. 1987). “The identical invention must be shown in as complete detail as is contained in the...claim.” Richardson v. Suzuki Motor Co., 868 F. 2d 1226, 1236, 9 U.S.P.Q. 2d 1913, 1920 (Fed. Cir. 1989). See also MPEP 2131.

Therefore, the claims of the present application are unpatentable as being anticipated by U.S. Patent No. 6,057,872 to Candelore. under 35 U.S.C. §102(e) only if Candelore teaches each and every element of the claims.

B. The Rejected Claims

Of the pending claims, claims 12-14, 34-36, 39-41 and 61-63 are independent. Each of the independent claims calls for either an electronic commerce system or a method of processing order acceptance requests in an electronic commerce system. In each case a client computer transmits an order acceptance request to a server computer associated with an electronic commerce system. The order acceptance request includes a plurality of modular elements whose individual integrity is protected by embedding cryptographic security codes within each modular element. Included among the plurality of modular elements is a digital coupon. As with the other modular elements, the digital coupon is individually protected by an embedded cryptographic security code.

The client computer is programmed to transmit an order acceptance request to the server. The server processes the order acceptance request based on pre-programmed criteria, including authentication of the cryptographic security codes embedded within each of the modular

elements, and examination of the contents of the modular elements. The server then sends an order acceptance response to the client based on the client's order acceptance request and pre-programmed order acceptance criteria. The order acceptance response also includes a plurality of modular elements whose individual integrity is protected by embedding cryptographic security codes within each of the modular elements. Candelore does not teach every element of the appealed claims.

Among the features of the pending claims which are not taught by Candelore is a client computer configured for, or the step of, transmitting an order acceptance request that includes a plurality of modular elements, with each modular element individually protected by an imbedded cryptographic security code. Also among the features of the pending claims is a server configured to, or the step of, transmitting an order acceptance response to a client, the order acceptance response also including a plurality of modular elements whose individual integrity is protected by embedding a cryptographic security code within each modular element.

Candelore teaches digital coupons for pay televisions, (see title). Candelore enables cable TV service providers to transmit credit information in the form of "digital coupons" to individual subscriber terminals to promote particular programs and reward viewer loyalty. (col. 1, lines 9-14). The digital coupon information allows the terminals to obtain credits when recovering particular programs as defined by preconditions of the digital coupon information (col. 3, lines 29-32). A user interface such as a graphical user interface may be provided to allow the subscriber to selectively redeem the credits for example, a user may have a variety of options from which to choose, where a cash balance and/or a coupon balance are redeemed in full or in part. (col. 3, lines 53-58). Various cryptographic techniques may also be employed to prevent unauthorized access to the digital coupons. (col. 4, lines 38-39). The digital coupons may be generated locally in the terminals, based on criteria sent by the service provider, or transmitted directly from the service provider as an entitlement from the service provider.

The communication system contemplated by Candelore is shown in Candelore's Fig. 1. The communication system includes a transmitting end 110, a channel 120, and a receiving end shown 130. (col. 5, lines 7-9). The channel 120 may comprise coaxial cable, optical fiber, and/or a wireless link such as a satellite or RT broadcast link. The transmitting end may be a cable television system headend, a satellite uplink center, or an RF broadcast center. (col. 5, lines 39-44). A controller 130 associated with the transmitting end causes digital coupon to be

encrypted and multiplexed along with program service data and control data. (col. 7, lines 19-23) the control data includes cryptographic data which is used for generating working keys at the terminals for decoding received data. (col. 7, lines 29-32)

The Examiner points to Candelore's communication channel 120 as teaching client and server computers connected by a public packet switched network. However, col. 5, lines 40-44 specifically define the communication channel

The channel 120 may be a coaxial cable, optical fiber, and/or a wireless link such as a satellite or RF broadcast link. The transmitting end may be a cable television system headend, a satellite uplink center, or an RF broadcast center, for example.

Nowhere is a public packet switched network disclosed or even hinted at in Candelore's disclosure. For this reason alone the pending claims are allowable over Candelore.

Nonetheless, even if Candelore's communication channel 120 is somehow interpreted as comprising a public packet switched network, several other features of the pending claims are also missing from the disclosure of Candelore.

First and foremost, Candelore does not teach transmitting an order acceptance request comprising a plurality of terms and conditions of a proposed offer for a purchase, the order acceptance request including a plurality of modular elements whose individual integrity is protected by embedding cryptographic security codes in each modular element. Candelore col. 5, lines 6-25 states only that the user terminals are able to communicate with a pay per view processing function and usage pattern accounting function via the communication channel. Nowhere does this passage describe a discrete message having a plurality of modular components where each component is individually protected by a cryptographic code. Similarly, Candelore col. 7, line 19 – col. 9, line 65, the other passage cited by the Examiner as teaching an order acceptance request as claimed in the present application, likewise fails to disclose an order acceptance request as described in the pending claims. At most, Candelore teaches a single modular element, a digital coupon, protected by an embedded cryptographic code. Nowhere does Candelore teach an order acceptance request that includes terms and conditions of a proposed offer. Nowhere does Candelore teach a discrete message including a plurality of modular elements. And nowhere does Candelore teach protecting the integrity of a plurality of modular elements by embedding cryptographic codes in each modular element.

Next, Candelore is even further from teaching or suggesting a step of transmitting an order acceptance response request from the server to the client, wherein the order acceptance response also includes a plurality of modular elements whose individual integrity is protected by embedding cryptographic security codes in each modular element. The Examiner points again to Candelore col. 5, lines 6-25 and col. 7, line 19 – col. 9, line 65. But again, nothing in these passages describe cryptographically protecting any modular elements other than a digital coupon. Candelore does not teach sending an order acceptance response that includes a plurality of individually protected modular elements Nothing in the teaching of Candelore even suggests the automated negotiation process set forth in the pending claims of the instant application.

Since Candelore fails to disclose all of the elements of any of the pending claims, all of the pending claims allowable over the teaching of Candelore, and the final rejection should be reversed.

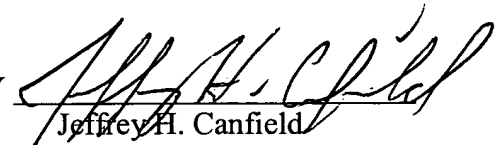
IX. CONCLUSION

U.S. Patent No. 6,057,872 to Candelore does not disclose every element of claims 12-36 and 39-63. Candelore does not anticipate the pending claims For these reasons Appellants respectfully submit that the rejection of pending claims is an error in law and in fact and should therefore be reversed by this Board.

Respectfully submitted,

BELL, BOYD & LLOYD LLC

BY



Jeffrey H. Canfield

Reg. No. 38,404

P.O. Box 1135

Chicago, Illinois 60690-1135

Phone: (312) 807-4233

Dated: September 7, 2004

APPENDIX

CLAIMS:

12. An electronic commerce system comprising:

a client computer; and

a server computer;

the client computer and the server computer being interconnected by a public packet switched communications network;

the client computer being programmed to transmit to the server computer an order acceptance request comprising a plurality of terms or conditions of a proposed offer for a purchase, the order acceptance request comprising a discrete message that includes a plurality of modular elements whose individual integrity is protected by embedding cryptographic security codes within each of the modular elements, at least one of the modular elements individually protected by a cryptographic security code being a digital coupon;

the server computer being programmed to process the order acceptance request based on pre-programmed criteria, including authentication of the cryptographic security codes embedded within each of the modular elements and examination of the modular elements of the discrete message individually protected by the cryptographic security codes, and, based on the processing of the order acceptance request, to transmit to the client computer an order acceptance response based on the pre-programmed criteria, the order acceptance response comprising a discrete message transmitted during a negotiation phase of a transaction that includes a plurality of modular elements whose individual integrity is protected by embedding cryptographic security codes within each of the modular elements;

wherein the client computer is programmed to receive the digital coupon, protected by a cryptographic security code, from another computer.

13. An electronic commerce system comprising:

a client computer; and

a server computer;

the client computer and the server computer being interconnected by a public packet switched communications network;

the client computer being programmed to transmit to the server computer an order acceptance request comprising a plurality of terms or conditions of a proposed offer for a purchase, the order acceptance request comprising a discrete message that includes a plurality of modular elements whose individual integrity is protected by embedding cryptographic security codes within each of the modular elements, at least one of the modular elements individually protected by a cryptographic security code being a digital coupon;

the server computer being programmed to process the order acceptance request based on pre-programmed criteria, including authentication of the cryptographic security codes embedded within each of the modular elements and examination of the modular elements of the discrete message individually protected by the cryptographic security codes, and, based on the processing of the order acceptance request, to transmit to the client computer an order acceptance response based on the pre-programmed criteria, the order acceptance response comprising a discrete message transmitted during a negotiation phase of a transaction that includes a plurality of modular elements whose individual integrity is protected by embedding cryptographic security codes within each of the modular elements;

wherein the digital coupon is configured to be used by any coupon holder that possesses the digital coupon, and wherein the server computer is programmed to accept the digital coupon without regard to the identity of the coupon holder.

14. An electronic commerce system comprising:

a client computer; and

a server computer;

the client computer and the server computer being interconnected by a public packet switched communications network;

the client computer being programmed to transmit to the server computer an order acceptance request comprising a plurality of terms or conditions of a proposed offer for a purchase, the order acceptance request comprising a discrete message that includes a plurality of modular elements whose individual integrity is protected by embedding cryptographic security codes within each of the modular elements, at least one of the modular elements individually protected by a cryptographic security code being a digital coupon;

the server computer being programmed to process the order acceptance request based on pre-programmed criteria, including authentication of the cryptographic security codes embedded within each of the modular elements and examination of the modular elements of the discrete message individually protected by the cryptographic security codes, and, based on the processing of the order acceptance request, to transmit to the client computer an order acceptance response based on the pre-programmed criteria, the order acceptance response comprising a discrete message transmitted during a negotiation phase of a transaction that includes a plurality of modular elements whose individual integrity is protected by embedding cryptographic security codes within each of the modular elements;

wherein the server computer is programmed to determine whether a coupon holder is authorized to use the digital coupon and to accept the digital coupon only if the coupon holder is authorized to use the digital coupon.

15. The electronic commerce system of claim 14 wherein the client computer is programmed to provide information to the server computer concerning identify of the coupon holder.

16. The electronic commerce system of claim 15 wherein the server computer is programmed to authenticate authority of the client computer by virtue of a two-way-authenticated SSL connection.

17. The electronic commerce system of claim 15 wherein the server computer is programmed to authenticate authority of the client computer using a basic authentication method.

18. The electronic commerce system of claim 15 wherein the server computer is programmed to authenticate authority of the client computer using a client certificate.

19. The electronic commerce system of claim 3 wherein the digital coupon contains a serial number to ensure that the digital coupon is used only once and the server computer is programmed to determine whether the digital coupon has been used previously and to accept the digital coupon only if it has not been used previously.

20. The electronic commerce system of claim 3 wherein the server computer is programmed to set at least one term of the order acceptance response based on whether the digital coupon is present in the order acceptance request.
21. The electronic commerce system of claim 20 wherein the at least one term of the order acceptance response is a price.
22. The electronic commerce system of claim 3 wherein the server computer is programmed to set at least one term of the order acceptance response based on whether the digital coupon in the order acceptance request is a particular type of digital coupon.
23. The electronic commerce system of claim 3 wherein the digital coupon is a gift certificate.
24. The electronic commerce system of claim 23 wherein the gift certificate comprises a serial number.
25. The electronic commerce system of claim 24 wherein the server computer is programmed to ensure that the serial number has been used only once by checking a database in which the serial number is stored.
26. The electronic commerce system of claim 23 wherein the client computer is programmed to display an icon of the gift certificate and to initiate the order acceptance request after a recipient of the gift certificate clicks on the icon.
27. The electronic commerce system of claim 26 further comprising a merchant computer, the merchant computer being programmed to respond to the recipient clicking on the icon by transmitting an order form to the client computer, the client computer being programmed to initiate the order acceptance request when the recipient fills in the order form.

28. The electronic commerce system of claim 23 wherein the client computer is a first client computer programmed to receive the gift certificate from a second client computer.

29. The electronic commerce system of claim 28 wherein the server computer is programmed to transmit the gift certificate to the second client computer, which in turn is programmed to forward the gift certificate to the first client computer.

30. The electronic commerce system of claim 29 wherein the gift certificate comprises a serial number and the server computer is programmed to create the serial number of the gift certificate before transmitting the gift certificate to the second client computer.

31. The electronic commerce system of claim 30 wherein the server computer is programmed to store the serial number in a database before transmitting the gift certificate to the second client computer, and is programmed, when it receives the gift certificate from the first client computer to ensure that the serial number has been used only once by checking the database in which the serial number is stored.

32. The electronic commerce system of claim 29 further comprising a merchant computer programmed to transmit the gift certificate to the server computer before the server computer transmits the gift certificate to the second client computer.

33. The electronic commerce system of claim 32 wherein the merchant computer is programmed to transmit the gift certificate to the server computer in the form of an order acceptance request that includes extension information indicating that the order acceptance request is a gift certificate.

34. An electronic commerce system comprising:
a client computer; and
a server computer;
the client computer and the server computer being interconnected by a public packet switched communications network;

the client computer being programmed to transmit to the server computer an order acceptance request comprising a plurality of terms or conditions of a proposed offer for a purchase, the order acceptance request comprising a discrete message that includes a plurality of modular elements whose individual integrity is protected by embedding cryptographic security codes within each of the modular elements, at least one of the modular elements individually protected by a cryptographic security code being a digital coupon;

the server computer being programmed to process the order acceptance request based on pre-programmed criteria, including authentication of the cryptographic security codes embedded within each of the modular elements and examination of the modular elements of the discrete message individually protected by the cryptographic security codes, and, based on the processing of the order acceptance request, to transmit to the client computer an order acceptance response based on the pre-programmed criteria, the order acceptance response comprising a discrete message transmitted during a negotiation phase of a transaction that includes a plurality of

modular elements whose individual integrity is protected by embedding cryptographic security codes within each of the modular elements;

wherein the cryptographic security codes are embedded within respective ones of the plurality of modular elements.

35. An electronic commerce system comprising:

a client computer; and

a server computer;

the client computer and the server computer being interconnected by a public packet switched communications network;

the client computer being programmed to transmit to the server computer an order acceptance request comprising a plurality of terms or conditions of a proposed offer for a purchase, the order acceptance request comprising a discrete message that includes a plurality of modular elements whose individual integrity is protected by embedding cryptographic security codes within each of the modular elements, at least one of the modular elements individually protected by a cryptographic security code being a digital coupon;

the server computer being programmed to process the order acceptance request based on pre-programmed criteria, including authentication of the cryptographic security codes embedded

within each of the modular elements and examination of the modular elements of the discrete message individually protected by the cryptographic security codes, and, based on the processing of the order acceptance request, to transmit to the client computer an order acceptance response based on the pre-programmed criteria, the order acceptance response comprising a discrete message transmitted during a negotiation phase of a transaction that includes a plurality of modular elements whose individual integrity is protected by embedding cryptographic security codes within each of the modular elements;

wherein the cryptographic security codes are digital signatures.

36. An electronic commerce system comprising:

a client computer; and

a server computer;

the client computer and the server computer being interconnected by a public packet switched communications network;

the client computer being programmed to transmit to the server computer an order acceptance request comprising a plurality of terms or conditions of a proposed offer for a purchase, the order acceptance request comprising a discrete message that includes a plurality of modular elements whose individual integrity is protected by embedding cryptographic security codes within each of the modular elements, at least one of the modular elements individually protected by a cryptographic security code being a digital coupon;

the server computer being programmed to process the order acceptance request based on pre-programmed criteria, including authentication of the cryptographic security codes embedded within each of the modular elements and examination of the modular elements of the discrete message individually protected by the cryptographic security codes, and, based on the processing of the order acceptance request, to transmit to the client computer an order acceptance response based on the pre-programmed criteria, the order acceptance response comprising a discrete message transmitted during a negotiation phase of a transaction that includes a plurality of modular elements whose individual integrity is protected by embedding cryptographic security codes within each of the modular elements;

wherein the cryptographic security codes are message authentication codes.

39. A method of processing order acceptance requests in an electronic commerce system, comprising a client computer and a server computer interconnected by a public packet switched communications network, the method comprising:

receiving at the server computer an order acceptance request transmitted by the client computer comprising a plurality of terms or conditions of a proposed offer for a purchase, the order acceptance request comprising a discrete message that includes a plurality of modular elements whose individual integrity is protected by cryptographic security codes embedded within each of the modular elements, at least one of the modular elements individually protected by a cryptographic security code being a digital coupon;

processing the order acceptance request based on pre-programmed criteria, including authentication of the cryptographic security codes and examination of the modular elements of the discrete message individually protected by the cryptographic security codes; and

based on the processing of the order acceptance request, transmitting to the client computer an order acceptance response based on the pre-programmed criteria, the order acceptance response comprising a discrete message transmitted during a negotiation phase of a transaction that includes a plurality of modular elements whose individual integrity is protected by cryptographic security codes embedded within each of the modular elements;

wherein the client computer receives the digital coupon, protected by a cryptographic security code, from another computer.

40. A method of processing order acceptance requests in an electronic commerce system, comprising a client computer and a server computer interconnected by a public packet switched communications network, the method comprising:

receiving at the server computer an order acceptance request transmitted by the client computer comprising a plurality of terms or conditions of a proposed offer for a purchase, the order acceptance request comprising a discrete message that includes a plurality of modular elements whose individual integrity is protected by cryptographic security codes embedded within each of the modular elements, at least one of the modular elements individually protected by a cryptographic security code being a digital coupon;

- processing the order acceptance request based on pre-programmed criteria, including authentication of the cryptographic security codes and examination of the modular elements of the discrete message individually protected by the cryptographic security codes; and

- based on the processing of the order acceptance request, transmitting to the client computer an order acceptance response based on the pre-programmed criteria, the order acceptance response comprising a discrete message transmitted during a negotiation phase of a transaction that includes a plurality of modular elements whose individual integrity is protected by cryptographic security codes embedded within each of the modular elements;

- wherein the digital coupon is configured to be used by any coupon holder that possesses the digital coupon, the method further comprising accepting the digital coupon at the server computer is programmed without regard to identity to the coupon holder.

41. A method of processing order acceptance requests in an electronic commerce system, comprising a client computer and a server computer interconnected by a public packet switched communications network, the method comprising:

- receiving at the server computer an order acceptance request transmitted by the client computer comprising a plurality of terms or conditions of a proposed offer for a purchase, the order acceptance request comprising a discrete message that includes a plurality of modular elements whose individual integrity is protected by cryptographic security codes embedded within each of the modular elements, at least one of the modular elements individually protected by a cryptographic security code being a digital coupon;

- processing the order acceptance request based on pre-programmed criteria, including authentication of the cryptographic security codes and examination of the modular elements of the discrete message individually protected by the cryptographic security codes; and

- based on the processing of the order acceptance request, transmitting to the client computer an order acceptance response based on the pre-programmed criteria, the order acceptance response comprising a discrete message transmitted during a negotiation phase of a transaction that includes a plurality of modular elements whose individual integrity is protected by cryptographic security codes embedded within each of the modular elements;

further comprising the steps of determining whether a coupon holder is authorized to use the digital coupon and accepting the digital coupon at the server computer only if the coupon holder is authorized to use the digital coupon.

42. The method of claim 41 further comprising receiving information at the server computer provided by the client computer concerning identify of the coupon holder.

43. The method of claim 42 further comprising authenticating authority of the client computer, at the server computer, by virtue of a two-way-authenticated SSL connection.

44. The method of claim 42 wherein authenticating authority of the client computer is performed using a basic authentication method.

45. The method of claim 42 wherein authenticating authority of the client computer is performed using a client certificate.

46. The method of claim 37 wherein the digital coupon contains a serial number to ensure that the digital coupon is used only once, the method further comprising determining at the server computer whether the digital coupon has been used previously and accepting the digital coupon only if it has not been used previously.

47. The method of claim 37 further comprising setting, at the server computer, at least one term of the order acceptance response based on whether the digital coupon is present in the order acceptance request.

48. The method of claim 47 wherein the at least one term of the order acceptance response is a price.

49. The method of claim 37 further comprising setting, at the server computer, at least one term of the order acceptance response based on whether the digital coupon in the order acceptance request is a particular type of digital coupon.

50. The method of claim 37 wherein the digital coupon is a gift certificate.
51. The method of claim 50 wherein the gift certificate comprises a serial number.
52. The method of claim 51 further comprising ensuring that the serial number has been used only once by checking a database at the server computer in which the serial number is stored.
53. The method of claim 50 wherein the client computer displays an icon of the gift certificate and initiates the order acceptance request after a recipient of the gift certificate clicks on the icon.
54. The method of claim 53 wherein the electronic commerce system further comprises a merchant computer and wherein the merchant computer responds to the recipient clicking on the icon by transmitting an order form to the client computer, and wherein the client computer initiates the order acceptance request when the recipient fills in the order form.
55. The method of claim 50 wherein the client computer is a first client computer that receive the gift certificate from a second client computer in the electronic commerce system.
56. The method of claim 55 further comprising transmitting the gift certificate from the server computer to the second client computer, which in turn forwards the gift certificate to the first client computer.
57. The method of claim 56 wherein the gift certificate comprises a serial number and wherein the method further comprises creating the serial number of the gift certificate at the server computer before transmitting the gift certificate to the second client computer.
58. The method of claim 56 further comprising storing the serial number in a database at the server computer before transmitting the gift certificate to the second client computer, and when the server computer receives the gift certificate from the first client computer, ensuring that the

serial number has been used only once by checking the database at the server computer in which the serial number is stored.

59. The method of claim 56 further wherein the electronic commerce system further comprises a merchant computer, the method further comprising receiving the gift certificate at the server computer from the merchant computer before transmitting the gift certificate from the server computer to the second client computer.

60. The method of claim 59 wherein the merchant computer transmits the gift certificate to the server computer in the form of an order acceptance request that includes extension information indicating that the order acceptance request is a gift certificate.

61. A method of processing order acceptance requests in an electronic commerce system, comprising a client computer and a server computer interconnected by a public packet switched communications network, the method comprising:

receiving at the server computer an order acceptance request transmitted by the client computer comprising a plurality of terms or conditions of a proposed offer for a purchase, the order acceptance request comprising a discrete message that includes a plurality of modular elements whose individual integrity is protected by cryptographic security codes embedded within each of the modular elements, at least one of the modular elements individually protected by a cryptographic security code being a digital coupon;

processing the order acceptance request based on pre-programmed criteria, including authentication of the cryptographic security codes and examination of the modular elements of the discrete message individually protected by the cryptographic security codes; and

based on the processing of the order acceptance request, transmitting to the client computer an order acceptance response based on the pre-programmed criteria, the order acceptance response comprising a discrete message transmitted during a negotiation phase of a transaction that includes a plurality of modular elements whose individual integrity is protected by cryptographic security codes embedded within each of the modular elements;

wherein the cryptographic security codes are embedded within respective ones of the plurality of modular elements.

62. A method of processing order acceptance requests in an electronic commerce system, comprising a client computer and a server computer interconnected by a public packet switched communications network, the method comprising:

receiving at the server computer an order acceptance request transmitted by the client computer comprising a plurality of terms or conditions of a proposed offer for a purchase, the order acceptance request comprising a discrete message that includes a plurality of modular elements whose individual integrity is protected by cryptographic security codes embedded within each of the modular elements, at least one of the modular elements individually protected by a cryptographic security code being a digital coupon;

processing the order acceptance request based on pre-programmed criteria, including authentication of the cryptographic security codes and examination of the modular elements of the discrete message individually protected by the cryptographic security codes; and

based on the processing of the order acceptance request, transmitting to the client computer an order acceptance response based on the pre-programmed criteria, the order acceptance response comprising a discrete message transmitted during a negotiation phase of a transaction that includes a plurality of modular elements whose individual integrity is protected by cryptographic security codes embedded within each of the modular elements;

wherein the cryptographic security codes are digital signatures.

63. A method of processing order acceptance requests in an electronic commerce system, comprising a client computer and a server computer interconnected by a public packet switched communications network, the method comprising:

receiving at the server computer an order acceptance request transmitted by the client computer comprising a plurality of terms or conditions of a proposed offer for a purchase, the order acceptance request comprising a discrete message that includes a plurality of modular elements whose individual integrity is protected by cryptographic security codes embedded within each of the modular elements, at least one of the modular elements individually protected by a cryptographic security code being a digital coupon;

processing the order acceptance request based on pre-programmed criteria, including authentication of the cryptographic security codes and examination of the modular elements of the discrete message individually protected by the cryptographic security codes; and

based on the processing of the order acceptance request, transmitting to the client computer an order acceptance response based on the pre-programmed criteria, the order acceptance response comprising a discrete message transmitted during a negotiation phase of a transaction that includes a plurality of modular elements whose individual integrity is protected by cryptographic security codes embedded within each of the modular elements;

wherein the cryptographic security codes are message authentication codes.

SUPPLEMENTAL APPENDIX

Exhibit 1: Final Office Action (Mailed on November 13, 2003)

Exhibit 2: U.S. Patent Number 6,057,872



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/054,180	04/01/1998	BRIAN J. REISTAD	06543035001	2217
24573	7590	11/13/2003		
BELL, BOYD & LLOYD, LLC PO BOX 1135 CHICAGO, IL 60690-1135				
			EXAMINER BACKER, FIRMIN	
			ART UNIT 3621	PAPER NUMBER

DATE MAILED: 11/13/2003

Due: 2/13/04

Please find below and/or attached an Office communication concerning this application or proceeding.

RECEIVED
BELL, BOYD & LLOYD
INTELLECTUAL PROPERTY DECKET
NOV 17 2003
ATTY RNB-JHC-JAE
DOCKET # 112948-64

Office Action Summary

Application No.

09/054,180

Applicant(s)

REISTAD ET AL.

Examiner

Firmin Backer

Art Unit

3621

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 08 October 2003.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 12-36 and 39-63 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 12-36 and 39-63 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on _____ is: a) ☐ approved b) ☐ disapproved by the Examiner.
If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
* See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____
- 4) ☐ Interview Summary (PTO-413) Paper No(s). _____
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____

Response to Request for Reconsideration

This is in response to a request for reconsideration file October 8th, 2003. Claims 12-36 and 39-63 are being reconsidered in this action.

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 12-36, 39-63 rejected under 35 U.S.C. 102(e) as being anticipated by Candelore (U.S. Patent No. 6,057,872).

3. As per claim 12, Candelore teaches an electronic commerce system (*transaction communication system,, fig 1*) comprising a client computer (*receiving end, 130*) and a server computer (*transmitting end, 110*), (*see fig 1*) the client computer and the server computer being interconnected (*channel, 120*) by a public packet switched communications network (*see fig 1, column 5 lines 6-25*), the client computer being programmed to transmit to the server computer an order acceptance request comprising a plurality of terms or conditions of a proposed offer for a purchase, the order acceptance request comprising a discrete message that includes a plurality of modular elements whose individual integrity is protected by embedding cryptographic

Art Unit: 3621

security codes within each of the modular elements, at least one of the modular elements individually protected by a cryptographic security code being a digital coupon (*see fig 1, 2, column 5 lines 6-25, 7 lines 19-9 line 65*), the server computer being programmed to process the order acceptance request based on pre-programmed criteria, including authentication of the cryptographic security codes embedded within each of the modular elements and examination of the modular elements of the discrete message individually protected by the cryptographic security codes, and, based on the processing of the order acceptance request, to transmit to the client computer an order acceptance response based on the pre-programmed criteria, the order acceptance response comprising a discrete message transmitted during a negotiation phase of a transaction that includes a plurality of modular elements whose individual integrity is protected by embedding cryptographic security codes within each of the modular elements, wherein the client computer is programmed to receive the digital coupon, protected by a cryptographic security code (*keys*), from another computer (*see fig 1, 2, column 5 lines 6-25, 7 lines 19-9 line 65*).

4. As per claim 13-36, 39-63, they disclose the same inventive concept as claim 12.

Therefore, they are rejected under the same rationale.

Response to Arguments

5. Applicant's arguments filed October 8th, 2003 have been fully considered but they are not persuasive.

a. Applicant argues that the prior art fail to teach an inventive concept wherein a negotiation process between a client and a server in which the client terminal sends a purchase order request to the server and the server send a response. Examiner respectfully disagrees with applicant's characterization with the prior art. Candelore teaches a user interface 226 enables a viewer to select program services for viewing on a television (TV) 180. If a user is authorized to receive the selected service by subscription, individual purchase (e.g., *pay per view*), or according to a digital coupon credit, the secure processor 220 will actuate the switch 218 to couple the decrypted output 216 from decryption processor 212 to the TV 180 via user interface 226. The digital coupon information may provide a discount when the user terminals order one or more PPV programs through the PPV order processing function 115. As an example, if a terminal orders five PPV programs within the current billing cycle, the digital coupon credit may allow the terminal to order a sixth PPV program at no charge. Or, for terminals that order PPV programs infrequently, the digital coupon credit may allow the terminal to order a first PPV program at half-price.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO**

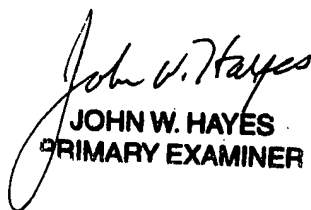
Art Unit: 3621

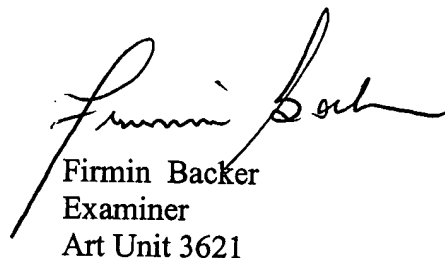
MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Firmin Backer whose telephone number is (703) 305-0624. The examiner can normally be reached on Mon-Thu 8:30-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James Trammell can be reached on (703) 305-9768. The fax phone numbers for the organization where this application or proceeding is assigned are (703) 305-7687 for regular communications and (703) 305-7687 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 308-1113.


JOHN W. HAYES
PRIMARY EXAMINER


Firmin Backer
Examiner
Art Unit 3621

November 11, 2003